



REC'D 23 FEB 2004

WIPO PCT

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 23 DEC. 2003

DOCUMENT DE PRIORITÉ

PRÉSENTÉ OU TRANSMIS
CONFORMÉMENT À LA
RÈGLE 17.1.a) OU b)

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

BEST AVAILABLE COPY

INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE

SIEGE
26 bis, rue de Saint Petersburg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr



26 bis, rue de Saint Pétersbourg
75900 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ
Code de la propriété intellectuelle - Livre VI

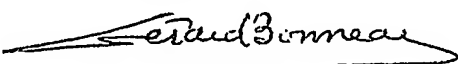


REQUÊTE EN DÉLIVRANCE 1/2

Cet imprimé est à remplir lisiblement à l'encre noire

08 540 W / 260899

REMISE DES PIÈCES DATE INPI-NICE, le 12 DEC. 2002 LIEU N° D'ENREGISTREMENT 0215740 NATIONAL ATTRIBUÉ PAR L'INPI DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 12 DEC. 2002		1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE CABINET BONNEAU Les Taissonnières HB3 1681, route des Dolines 06560 Sophia Antipolis	
Vos références pour ce dossier (facultatif) ASK/B24/02			
Confirmation d'un dépôt par télécopie <input type="checkbox"/> N° attribué par l'INPI à la télécopie			
2 NATURE DE LA DEMANDE		Cochez l'une des 4 cases suivantes	
Demande de brevet		<input checked="" type="checkbox"/>	
Demande de certificat d'utilité		<input type="checkbox"/>	
Demande divisionnaire		<input type="checkbox"/>	
Demande de brevet initiale		N°	Date
ou demande de certificat d'utilité initiale		N°	Date
Transformation d'une demande de brevet européen		<input type="checkbox"/>	
Demande de brevet initiale		N°	Date
3 TITRE DE L'INVENTION (200 caractères ou espaces maximum) Procédé sécurisé de modification de données enregistrées dans une carte à mémoire			
4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE		Pays ou organisation Date N° Pays ou organisation Date N° Pays ou organisation Date N° <input type="checkbox"/> S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»	
5 DEMANDEUR		<input type="checkbox"/> S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite»	
Nom ou dénomination sociale		ASK	
Prénoms			
Forme juridique		S.A.	
N° SIREN		4 . 1 . 3 . 9 . 6 . 7 . 1 . 5 . 9	
Code APE-NAF		3 . 0 . 0 . C	
Adresse	Rue	Les Bouillides 15, traverse des Brucs	
	Code postal et ville	06560	VALBONNE
Pays		France	
Nationalité		Française	
N° de téléphone (facultatif)			
N° de télécopie (facultatif)			
Adresse électronique (facultatif)			

REMISE DES PIÈCES DATE LIEU N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI		Réservé à l'INPI INPI-NICE, le 12 DEC. 2002 0215740		DB 540 W / 260899
Vos références pour ce dossier : <i>(facultatif)</i>		ASK/B24/02		
6 MANDATAIRE				
Nom		BONNEAU		
Prénom		Gérard		
Cabinet ou Société		CABINET BONNEAU		
N° de pouvoir permanent et/ou de lien contractuel		921030		
Adresse	Rue	Les Taissonnières HB3 1681, route des Dolines		
	Code postal et ville	06560	Sophia Antipolis	
N° de téléphone <i>(facultatif)</i>		04 93 00 01 66		
N° de télécopie <i>(facultatif)</i>		04 93 00 06 95		
Adresse électronique <i>(facultatif)</i>		cabinet.bonneau@wanadoo.fr		
7 INVENTEUR (S)				
Les inventeurs sont les demandeurs		<input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non Dans ce cas fournir une désignation d'inventeur(s) séparée		
8 RAPPORT DE RECHERCHE		Uniquement pour une demande de brevet (y compris division et transformation)		
Établissement immédiat ou établissement différé		<input checked="" type="checkbox"/> <input type="checkbox"/>		
Paiement échelonné de la redevance		Paiement en trois versements, uniquement pour les personnes physiques <input type="checkbox"/> Oui <input type="checkbox"/> Non		
9 RÉDUCTION DU TAUX DES REDEVANCES		Uniquement pour les personnes physiques <input type="checkbox"/> Requête pour la première fois pour cette invention (<i>joindre un avis de non-imposition</i>) <input type="checkbox"/> Requête antérieurement à ce dépôt (<i>joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence</i>) :		
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes				
10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire)  Gérard Bonneau-Mandataire N° 921030		VISA DE LA PRÉFECTURE OU DE L'INPI I.N.P.I. 249, rue Fernand Léger Sophia Antipolis 06560 VALBONNE		

La présente invention concerne les systèmes dans lesquels une partie des enregistrements de données mémorisés dans une carte à mémoire est modifiée lors d'une transaction effectuée avec un lecteur de la carte et
5 concerne plus particulièrement un procédé sécurisé de modification de données enregistrées dans une carte à mémoire lors d'une transaction avec un lecteur.

Les cartes à mémoire encore appelées cartes à puce sont de plus en plus utilisées comme support de données
10 associées aux titulaires des cartes. Parmi ces cartes, les cartes sans contact pour lesquelles l'échange d'informations se fait par couplage électromagnétique sans contact entre une antenne logée dans la carte et un lecteur associé ont été développées comme cartes d'accès à des
15 zones d'accès contrôlé, ou comme porte-monnaie électroniques.

D'une manière générale, les cartes à mémoire utilisent des mémoires non volatiles, effaçables et ré-inscriptibles du type EEPROM ou flash EPROM, de sorte que
20 les données restent inscrites dans la mémoire même lorsque cette dernière est hors tension. Elles permettent en outre une mise à jour des données enregistrées par effacement d'un ou plusieurs emplacements de mémoire et écriture de nouvelles données.

Il peut arriver que, lors d'une transaction, la mémoire soit corrompue en raison d'une interruption accidentelle de l'alimentation électrique due généralement à un "arrachement" de la carte, c'est à dire un retrait de celle-ci avant la fin du traitement, qui entraîne la perte
30 des données antérieures sans enregistrement de nouvelles données. Ce risque est particulièrement élevé avec les cartes du type sans contact où les limites de l'espace dans lequel la carte peut fonctionner correctement ne sont pas perceptibles.

Un risque supplémentaire se présente dans le cas des
35 mémoires non volatiles de type EEPROM avec lesquelles, si l'on interrompt une opération d'écriture avant sa fin

normale, il peut se faire que les données soient néanmoins écrites, et puissent donc être correctement lues peu après l'écriture. Toutefois, si l'on réitère cette lecture plus tard, il n'est pas certain que l'on puisse l'effectuer
5 correctement, car la rétention de l'information dans la cellule mémoire aura été insuffisante du fait de l'écriture interrompue avant terme.

Pour assurer l'intégrité des données, il est donc souhaitable que les cartes soient protégées à l'encontre de
10 tels risques, en garantissant que les données sont soit dans l'état modifié, soit dans l'état avant demande de modification, mais jamais dans un état intermédiaire indéterminé résultant d'un "arrachement".

Pour des raisons de sécurité de la transaction, il
15 est indispensable de recommencer toute la transaction si une coupure d'alimentation vient à se produire durant le cours de la transaction, sous peine de perdre irrémédiablement des données sensibles (par exemple le solde créditeur d'un porte-monnaie électronique) s'il n'est
20 pas possible de repartir du début de la transaction.

De manière à apporter une réponse au problème énoncé ci-dessus on a songé à mémoriser l'enregistrement de données dans une mémoire tampon avant de procéder à sa modification. Lorsque toutes les modifications ont été
25 apportées aux enregistrements à modifier, les anciens enregistrements sont effacés de la mémoire tampon.

Malheureusement, cette méthode nécessite pour chaque enregistrement une opération de sauvegarde dans la zone tampon, une opération d'effacement de l'enregistrement à
30 modifier, une opération de ré-écriture et une opération d'effacement de l'enregistrement ancien dans la zone tampon, soit 4 opérations au total. Cette opération a donc l'inconvénient de prendre beaucoup de temps ce qui représente un inconvénient majeur avec les cartes sans
35 contact.

En outre, la sauvegarde des données dans un autre emplacement de la mémoire avant d'effacer les données

antérieures nécessite la présence d'un "drapeau" (flag) destiné à indiquer que l'opération de modification s'est effectuée correctement ou non selon la valeur du drapeau. Le drapeau peut être un seul bit qui prend la valeur 0 ou 1 selon que la modification s'est déroulée correctement ou non. Dans la mesure où il n'est pas concevable pour des raisons évidentes d'enregistrer des bits de contrôle au même emplacement que les données, la seule solution consiste à enregistrer le drapeau (le ou les bits de contrôle) dans un emplacement de mémoire réservé à cet effet et donc un bloc entier de 16 ou 32 bits alors qu'un seul bit ou quelques bits suffisent.

Les inconvénients cités ci-dessus prennent encore plus d'importance lorsque la carte à mémoire est utilisée dans certaines applications ne nécessitant qu'une mémoire de faible capacité où il devient impératif de ne pas gaspiller des positions de la mémoire et dans lesquelles la valeur des données modifiées à chaque transaction est une fonction monotone dans le temps. Dans de telles applications, l'enregistrement de données en mémoire est soit un compteur croissant qui s'incrémente dans le temps comme par exemple une machine à photocopier, soit un compteur décroissant dans le cas d'une carte pour transport en commun où la valeur de l'enregistrement est décrémentée d'une unité à chaque voyage, soit un porte-monnaie électronique où la valeur de l'enregistrement ne peut aller qu'en décroissant.

C'est pourquoi le but de l'invention est de réaliser un procédé de modification de données dans une carte à mémoire lors d'une transaction qui s'effectue dans un minimum de temps compatible avec le temps d'accès limité à la carte durant la transaction.

Un autre but de l'invention est de réaliser un procédé de modification de données dans une carte à mémoire du type carte sans contact qui ne nécessite pas la réservation de bits de contrôle (drapeau) dans un emplacement de la mémoire.

L'objet de l'invention est donc un procédé modification des données dans un système de transaction par carte comprenant une carte à mémoire ou équivalent et un lecteur apte à lire la carte lorsque celle-ci se trouve dans une position déterminée par rapport au lecteur, la
 5 carte comprenant une mémoire non volatile, effaçable et ré-inscriptible comportant au moins un emplacement pour enregistrer une valeur de données en relation avec les transactions effectuées par la carte, chaque transaction
 10 entraînant la modification de la valeur de données, cette dernière étant une fonction monotone dans le temps. A chaque transaction, une opération d'écriture de la valeur de données effectue l'écriture de la nouvelle valeur de données dans un premier emplacement parmi deux emplacements
 15 prédéfinis formant un compteur dans la mémoire, l'opération d'écriture effectuant l'effacement de l'ancienne valeur de données enregistrée dans le deuxième emplacement de sorte qu'à la fin de l'opération d'écriture effectuée correctement le premier emplacement contient la nouvelle
 20 valeur de donnée alors que le deuxième emplacement contient la valeur zéro.

Les buts, objets et caractéristiques de l'invention apparaîtront plus clairement à la lecture de la description qui suit faite en référence aux dessins dans lesquels :

- 25 • La figure 1 est une représentation schématique de la mémoire d'une carte à mémoire dans laquelle est mis en œuvre le procédé selon l'invention,
- La figure 2 est une représentation schématique du contenu du compteur à deux étages de la mémoire pour
 30 chaque phase de l'opération d'écriture,
- La figure 3 est une représentation schématique du compteur à deux étages de la carte à mémoire pour chaque phase de l'opération de ré-écriture dans une première situation après arrachement,
- 35 • La figure 4 est une représentation schématique du compteur à deux étages de la carte à mémoire pour

chaque phase de l'opération de ré-écriture dans une deuxième situation après arrachement,

- La figure 5 est une représentation schématique du compteur à deux étages de la carte à mémoire pour chaque phase de l'opération de ré-écriture dans une troisième situation après arrachement,

- La figure 6 est une représentation schématique du compteur à deux étages de la carte à mémoire pour chaque phase de l'opération de ré-écriture dans une quatrième situation après arrachement, et

- La figure 7 est une représentation schématique du compteur à deux étages de la carte à mémoire pour chaque phase de l'opération de ré-écriture dans une cinquième situation après arrachement.

Dans une carte à puce du type mémoire à logique câblée utilisée dans les applications nécessitant peu de mémoire, les emplacements de mémoire sont comptés. Ainsi, la mémoire d'une telle carte à puce illustrée sur la figure 1 est une mémoire du type EEPROM ayant une capacité de 32 mots de 16 bits. L'invention décrite ci-dessous permet d'éviter de disposer dans la mémoire d'une zone de contrôle obligeant à réserver un mot entier. Pour cela, deux emplacements de mémoire formant un compteur à deux étages (étage A, étage B) sont réservés à l'enregistrement de la nouvelle valeur de données à chaque transaction effectuée entre le lecteur et la carte à mémoire.

Les principes de l'invention sont mis à profit dans toutes les applications où la valeur de données modifiée à chaque transaction est une fonction monotone dans le temps.

Dans certains cas (par exemple carte utilisée pour effectuer des photocopies), la valeur enregistrée est incrémentée alors que dans d'autres applications telles que l'accès à des zones d'accès contrôlé ou le porte-monnaie électronique, la valeur de données va en décroissant.

Cependant, il est préférable d'utiliser une incrémentation plutôt qu'une décrémentation du compteur. En effet, lorsqu'il y a arrachement, le risque est qu'il n'y ait pas

un rétention correcte des bites qui ont été écrits en mémoire. Dans ce cas, la valeur enregistrée peut diminuer parce que chaque bit 1 peut retomber à 0. Si on utilise une décrémentation, la valeur mal écrite allant en décroissant, sa décroissance fait courir un risque au titulaire de la carte dans la mesure où il n'est pas possible de savoir si la valeur en mémoire résulte d'une décrémentation normale ou d'une décroissance anormale du contenu de la mémoire. Au contraire, lorsqu'on "utilise" l'incrémentation, la décroissance de la mémoire ne présente pas de risque dans la mesure où la valeur à prendre en considération est la valeur précédente avant incrémentation lorsqu'il y a décroissance de la valeur mal enregistrée suite à un arrachement.

Dans le cas d'une décrémentation, il est aisé de considérer à chaque fois le complément à deux en binaire de la valeur de données. Ainsi, dans ce qui suit, la valeur de données est incrémentée à chaque transaction quelle que soit l'application considérée.

Le procédé selon l'invention consiste à enregistrer la nouvelle valeur de données qui a fait l'objet de la modification dans l'étage du compteur qui contenait la valeur 0 et à effacer l'autre étage du compteur pour mettre sa valeur à 0. Ces deux phases qui ne peuvent pas être inversées, sont déclenchées par une instruction d'écriture de la nouvelle valeur provenant du lecteur au moment de la transaction.

La figure 2 illustre le déroulement normal des opérations. Au départ, la lecture du compteur fait apparaître la valeur X dans l'étage A et la valeur 0 dans l'étage B. L'instruction d'écriture effectue ensuite l'écriture de la nouvelle valeur Y dans l'étage B, puis l'effacement de la valeur X de l'étage A. Donc, le compteur est incrémenté en une seule instruction.

Malheureusement, un arrachement de la carte peut se produire durant la transaction, en particulier lorsque la carte à puce est une carte sans contact. Dans ce cas

l'opération d'écriture ne se déroule pas correctement et soit l'écriture de la nouvelle valeur ne s'est pas faite correctement, soit l'ancienne valeur n'a pas été effacée. Dans ce cas, la transaction n'aboutit pas ou n'est pas validée. Ceci peut avoir comme résultat de ne pas autoriser l'ouverture d'un portillon d'accès à une zone à accès contrôlée ou de ne pas permettre un achat par un terminal de commerçant dans le cas d'un porte-monnaie électronique.

Le titulaire de la carte recommence alors l'opération consistant à faire passer sa carte dans ou devant un lecteur:---Celui-ci effectue en premier la lecture du compteur qui fait apparaître qu'aucun des deux étages du compteur n'est à la valeur 0. Il en déduit immédiatement qu'il y a eu arrachement et procède alors à la réparation du compteur comme décrit ci-dessous.

Les figures 3 à 7 illustrent les opérations de réparation du compteur lorsqu'il y a eu arrachement selon que cet arrachement s'est produit pendant la phase d'écriture, entre la phase d'écriture et la phase d'effacement ou pendant la phase d'effacement.

Dans une première situation illustrée par la figure 3, l'arrachement a eu lieu pendant la phase d'écriture, la valeur Y a été écrite mais la valeur X n'a pas été effacée. Dans ce cas, et bien que la valeur Y soit correcte, il n'est pas possible de garantir la rétention de cette valeur dans l'étage B. La valeur Y est donc ré-écrite avant de procéder à l'effacement de la valeur X de l'étage A pour la mettre à 0. A noter que l'écriture d'un emplacement de mémoire est une fonction OU entre la valeur qui s'y trouve et la nouvelle valeur et que par conséquent, on ne peut qu'écrire une nouvelle valeur que si l'ancienne valeur est égale à 0 ou à identiquement la nouvelle valeur (ce qui est le cas ici).

Dans une deuxième situation illustrée sur la figure 4, l'arrachement a eu lieu pendant la phase d'écriture, une valeur Y' comprise entre X et Y a été écrite dans l'étage B et la valeur X n'a pas été effacée de l'étage A. Dans ce

cas, une première opération d'écriture procède à la ré-écriture de Y' dans l'étage B et à l'effacement de X de l'étage A. Puis une opération d'écriture procède à l'écriture de Y dans l'étage A et à l'effacement de Y' de l'étage B, de sorte que le compteur se retrouve dans une situation normale où un étage contient la nouvelle valeur et où l'autre étage est à 0.

Dans une troisième situation illustrée sur la figure 5, l'arrachement a eu lieu pendant la phase d'écriture, une valeur Y' inférieure à X a été écrite dans l'étage B et la valeur X n'a pas été effacée. Dans ce cas, une première opération de ré-écriture procède à la ré-écriture de la valeur X dans l'étage A et à l'effacement de Y' de l'étage B. Ceci se justifie par le fait que la réparation du compteur s'effectue toujours avec la valeur la plus grande qui est, en l'occurrence, la valeur X. Puis une opération d'écriture procède à l'écriture de la valeur Y dans l'étage B et à l'effacement de X de l'étage A.

Dans une quatrième situation illustrée sur la figure 6, l'arrachement a eu lieu entre la phase d'écriture et la phase d'effacement, la valeur Y a été enregistrée dans l'étage B mais la valeur X n'a pas été effacée de l'étage A. Comme on ne peut pas garantir la rétention de la valeur Y, une opération de ré-écriture procède à la ré-écriture de la valeur Y dans l'étage B et à l'effacement de la valeur X de l'étage A.

Dans une cinquième situation illustrée sur la figure 7, l'arrachement a eu lieu pendant la phase d'effacement, la valeur Y a été écrite dans l'étage B mais la valeur X n'a pas été effacée correctement et une valeur X' se trouve dans l'étage A. Il faut donc procéder à une opération de ré-écriture de la valeur Y dans l'étage B qui permet alors l'effacement de la valeur X' de l'étage A.

Dans toutes les situations qui viennent d'être décrites, la réparation du compteur a été entreprise parce qu'aucun des deux étages ne contenait la valeur 0, et après réparation, l'un des deux étages contient la nouvelle

valeur de données alors que l'autre étage contient 0. A noter que, dans aucune des situations, le compteur se retrouve dans un état où la valeur maximale se trouvant dans l'étage A ou dans l'étage B est inférieure à
5 l'ancienne valeur (X).

REVENDICATIONS

1. Procédé de modification des données dans un système de transaction par carte comprenant une carte à mémoire ou équivalent et un lecteur apte à lire ladite carte lorsque celle-ci se trouve dans une position déterminée par rapport audit lecteur, ladite carte comprenant une
5 mémoire non volatile, effaçable et ré-inscriptible comportant au moins un emplacement pour enregistrer une valeur de données en relation avec les transactions effectuées par ladite carte, chaque transaction
10 entraînant la modification de ladite valeur de données, cette dernière étant une fonction monotone dans le temps,

ledit procédé étant caractérisé en ce que, à chaque transaction, une opération d'écriture de ladite
15 valeur de données effectue l'écriture de la nouvelle valeur de données (Y) dans un premier emplacement (B) parmi deux emplacements prédéfinis formant un compteur dans ladite mémoire, ladite opération d'écriture effectuant l'effacement de l'ancienne valeur de données
20 (X) enregistrée dans le deuxième emplacement (A) desdits deux emplacements de sorte qu'à la fin de l'opération d'écriture effectuée correctement ledit premier emplacement contient ladite nouvelle valeur de donnée alors que ledit deuxième emplacement contient la
25 valeur zéro.

2. Procédé selon l'une des revendications 1 à 7, dans lequel la valeur de données enregistrée dans un desdits
30 deux emplacements (A ou B) est incrémentée à chaque opération d'écriture.

3. Procédé selon la revendication 2, dans laquelle la transaction n'est pas validée du fait que ladite
35 opération d'écriture ne s'est pas effectuée correctement à cause d'un arrachement de ladite carte

REVENDECATIONS

1. Procédé de modification des données dans un système de transaction par carte comprenant une carte à mémoire ou équivalent et un lecteur apte à lire ladite carte lorsque celle-ci se trouve dans une position déterminée par rapport audit lecteur, ladite carte comprenant une mémoire non volatile, effaçable et ré-inscriptible comportant au moins un emplacement pour enregistrer une valeur de données en relation avec les transactions effectuées par ladite carte, — chaque transaction entraînant la modification de ladite valeur de données, cette dernière étant une fonction monotone dans le temps;

ledit procédé étant caractérisé en ce que, à chaque transaction, une opération d'écriture de ladite valeur de données effectue l'écriture de la nouvelle valeur de données (Y) dans un premier emplacement (B) parmi deux emplacements prédéfinis formant un compteur dans ladite mémoire, ladite opération d'écriture effectuant l'effacement de l'ancienne valeur de données (X) enregistrée dans le deuxième emplacement (A) desdits deux emplacements de sorte qu'à la fin de l'opération d'écriture effectuée correctement ledit premier emplacement contient ladite nouvelle valeur de donnée alors que ledit deuxième emplacement contient la valeur zéro.

2. Procédé selon la revendication 1, dans lequel la valeur de données enregistrée dans un desdits deux emplacements (A ou B) est incrémentée à chaque opération d'écriture.

3. Procédé selon la revendication 2, dans laquelle la transaction n'est pas validée du fait que ladite opération d'écriture ne s'est pas effectuée correctement à cause d'un arrachement de ladite carte

au cours de la transaction, aucun des deux étages dudit compteur n'ayant enregistré une valeur égale à zéro.

4. Procédé selon la revendication 2, comprenant en outre
5 une réparation dudit compteur par une opération de ré-écriture consistant à ré-écrire ladite nouvelle valeur (Y) dans ledit premier emplacement (B) et à effacer ladite ancienne valeur (X) dudit deuxième emplacement (A) lorsque l'arrachement a eu lieu pendant la phase
10 d'écriture de ladite nouvelle valeur.
5. Procédé selon la revendication 2, comprenant en outre, lorsque ledit premier emplacement (B) contient une valeur incorrecte (Y') comprise entre ladite ancienne
15 valeur de donnée (X) et ladite nouvelle valeur de données (Y), une réparation dudit compteur par une opération de ré-écriture consistant à ré-écrire ladite valeur incorrecte dans ledit premier emplacement et à effacer ladite ancienne valeur dudit deuxième
20 emplacement, suivie d'une opération d'écriture consistant à écrire ladite nouvelle valeur dans ledit deuxième emplacement (A) et à effacer ladite valeur incorrecte dudit premier emplacement.
- 25 6. Procédé selon la revendication 2, comprenant en outre, lorsque ledit premier emplacement (B) contient une valeur de données incorrecte (Y') inférieure à ladite ancienne valeur (X), une réparation dudit compteur par une opération de ré-écriture consistant à ré-écrire
30 ladite ancienne valeur de données (X) dans ledit deuxième emplacement (A) et à effacer ladite valeur de données incorrecte, suivie d'une opération d'écriture, consistant à écrire ladite nouvelle valeur de données (y) dans ledit premier emplacement et à effacer ladite
35 ancienne valeur de données dudit deuxième emplacement.

au cours de la transaction, aucun des deux étages dudit compteur n'ayant enregistré une valeur égale à zéro.

- 5 4. Procédé selon la revendication 2, comprenant en outre une réparation dudit compteur par une opération de ré-écriture consistant à ré-écrire ladite nouvelle valeur (Y) dans ledit premier emplacement (B) et à effacer ladite ancienne valeur (X) dudit deuxième emplacement (A) lorsque l'arrachement a eu lieu pendant la phase
10 d'écriture de ladite nouvelle valeur.
- 15 5. Procédé selon la revendication 2, comprenant en outre, lorsque ledit premier emplacement (B) contient une valeur incorrecte (Y') comprise entre ladite ancienne valeur de donnée (X) et ladite nouvelle valeur de données (Y), une réparation dudit compteur par une
20 opération de ré-écriture consistant à ré-écrire ladite valeur incorrecte dans ledit premier emplacement et à effacer ladite ancienne valeur dudit deuxième emplacement, suivie d'une opération d'écriture consistant à écrire ladite nouvelle valeur dans ledit
25 deuxième emplacement (A) et à effacer ladite valeur incorrecte dudit premier emplacement.
- 30 6. Procédé selon la revendication 2, comprenant en outre, lorsque ledit premier emplacement (B) contient une valeur de données incorrecte (Y') inférieure à ladite ancienne valeur (X), une réparation dudit compteur par une opération de ré-écriture consistant à ré-écrire
35 ladite ancienne valeur de données (X) dans ledit deuxième emplacement (A) et à effacer ladite valeur de données incorrecte, suivie d'une opération d'écriture, consistant à écrire ladite nouvelle valeur de données (y) dans ledit premier emplacement et à effacer ladite ancienne valeur de données dudit deuxième emplacement.

7. Procédé selon la revendication 2, comprenant en outre une réparation dudit compteur par une opération de ré-écriture consistant à ré-écrire ladite nouvelle valeur de données (Y) dans ledit premier emplacement (B) et à effacer ladite ancienne valeur de données (X) dudit deuxième emplacement (A) lorsque l'arrachement a eu lieu entre la phase d'écriture de ladite nouvelle valeur de données et la phase d'effacement de ladite ancienne valeur de données.

8. Procédé selon la revendication 2, comprenant en outre, lorsque l'arrachement a eu lieu pendant la phase d'effacement de ladite ancienne valeur de données (X) et qu'une valeur de données incorrecte (X') est enregistrée dans ledit deuxième emplacement (A), une réparation dudit compteur par une opération de ré-écriture consistant à ré-écrire ladite nouvelle valeur de données (Y) dans ledit premier emplacement (B) et à effacer ladite valeur de données incorrecte dudit deuxième emplacement.

9. Système de transaction par carte comprenant une carte à mémoire ou équivalent et un lecteur apte à lire ladite carte lorsque celle-ci se trouve dans une position déterminée par rapport audit lecteur, ladite carte incluant une mémoire non volatile, effaçable et ré-inscriptible comportant au moins un emplacement pour enregistrer une valeur de données en relation avec les transactions effectuées par ladite carte, chaque transaction entraînant la modification de ladite valeur de données, cette dernière étant une fonction monotone dans le temps ;

ledit système étant caractérisé en ce que ladite mémoire comprend un premier emplacement et un deuxième emplacement prédéfinis formant un compteur, chaque transaction donnant lieu à une instruction d'écriture effectuant l'écriture d'une nouvelle valeur de données

7. Procédé selon la revendication 2, comprenant en outre une réparation dudit compteur par une opération de ré-écriture consistant à ré-écrire ladite nouvelle valeur de données (Y) dans ledit premier emplacement (B) et à effacer ladite ancienne valeur de données (X) dudit deuxième emplacement (A) lorsque l'arrachement a eu lieu entre la phase d'écriture de ladite nouvelle valeur de données et la phase d'effacement de ladite ancienne valeur de données.

10

8. Procédé selon la revendication 2, comprenant en outre, lorsque l'arrachement a eu lieu pendant la phase d'effacement de ladite ancienne valeur de données (X) et qu'une valeur de données incorrecte (X') est enregistrée dans ledit deuxième emplacement (A), une réparation dudit compteur par une opération de ré-écriture consistant à ré-écrire ladite nouvelle valeur de données (Y) dans ledit premier emplacement (B) et à effacer ladite valeur de données incorrecte dudit deuxième emplacement.

15

20

9. Système de transaction par carte comprenant une carte à mémoire ou équivalent et un lecteur apte à lire ladite carte lorsque celle-ci se trouve dans une position déterminée par rapport audit lecteur, ladite carte incluant une mémoire non volatile, effaçable et ré-inscriptible comportant au moins un emplacement pour enregistrer une valeur de données en relation avec les transactions effectuées par ladite carte, chaque transaction entraînant la modification de ladite valeur de données, cette dernière étant une fonction monotone dans le temps ;

25

30

35

ledit système étant caractérisé en ce que ladite mémoire comprend un premier emplacement et un deuxième emplacement prédéfinis formant un compteur, chaque transaction donnant lieu à une instruction d'écriture effectuant l'écriture d'une nouvelle valeur de données

(Y) dans ledit premier emplacement (B) et l'effacement de l'ancienne valeur de données (X) dudit deuxième emplacement (A), de sorte qu'à la fin de l'opération d'écriture ledit premier emplacement contient ladite
5 nouvelle valeur de données alors que ledit deuxième emplacement contient la valeur zéro.

10. Système selon la revendication 8, dans lequel ladite carte à mémoire est une carte sans contact.

(Y) dans ledit premier emplacement (B) et l'effacement de l'ancienne valeur de données (X) dudit deuxième emplacement (A), de sorte qu'à la fin de l'opération d'écriture ledit premier emplacement contient ladite nouvelle valeur de données alors que ledit deuxième emplacement contient la valeur zéro.

- 5 10. Système selon la revendication 9, dans lequel ladite carte à mémoire est une carte sans contact.

ADRESSE	SEIZE BITS PAR MOT
0	NUMERO DE SERIE
1	
2	
3	
4	
5	ZONE 1
6	
7	
8	
9	
10	ZONE 2
11	
12	
13	
14	
15	
16	
17	
18	COMPTEUR ETAGE A
19	COMPTEUR ETAGE B
20	ZONE 3
21	
22	
23	
24	
25	
26	
27	
28	
29	ZONE 4
30	
31	

FIG. 1

ETAGE A	X
ETAGE B	0



ETAGE A	X
ETAGE B	Y



ETAGE A	0
ETAGE B	Y

OPERATION
D'ECRITURE

FIG. 2

2/4

ETAGE A	X
ETAGE B	Y



ETAGE A	X
ETAGE B	Y



ETAGE A	0
ETAGE B	Y

OPERATION
DE RE-ECRITURE

FIG. 3

ETAGE A	X
ETAGE B	Y'



ETAGE A	X
ETAGE B	Y'



ETAGE A	0
ETAGE B	Y'

OPERATION
DE RE-ECRITURE



ETAGE A	Y
ETAGE B	Y'



ETAGE A	Y
ETAGE B	0

OPERATION
D'ECRITURE

FIG. 4

3/4

ETAGE A	X
ETAGE B	Y'



ETAGE A	X
ETAGE B	Y'



ETAGE A	X
ETAGE B	0

OPERATION
DE RE-ECRITURE



ETAGE A	X
ETAGE B	Y



ETAGE A	0
ETAGE B	Y

OPERATION
D'ECRITURE

FIG. 5

ETAGE A	X
ETAGE B	Y



ETAGE A	X
ETAGE B	Y



ETAGE A	0
ETAGE B	Y

OPERATION
DE RE-ECRITURE

FIG. 6

ETAGE A	X'
ETAGE B	Y



ETAGE A	X'
ETAGE B	Y



ETAGE A	0
ETAGE B	Y

OPERATION
DE RE-ECRITURE

FIG. 7



BREVET D'INVENTION
CERTIFICAT D'UTILITÉ
Code de la propriété intellectuelle - Livre VI


N° 11 235 02

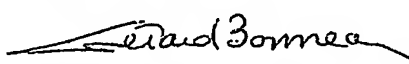
DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

DÉSIGNATION D'INVENTEUR(S) Page N° 1. / 1..
(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

Cet imprimé est à remplir lisiblement à l'encre noire

09 113 W / 260899

Vos références pour ce dossier (facultatif)		ASK/B24/02	
N° D'ENREGISTREMENT NATIONAL		02 15 740	
TITRE DE L'INVENTION (200 caractères ou espaces maximum) Procédé sécurisé de modification de données enregistrées dans une carte à mémoire			
LE(S) DEMANDEUR(S) : ASK Les Bouillides 15, traverse des Brucs 06560 VALBONNE			
DESIGNE(NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).			
Nom		PANGAUD	
Prénoms		Nicolas	
Adresse	Rue	Les Vergers des Belles Terres 481, route de Nice	
	Code postal et ville	06560	VALBONNE
Société d'appartenance (facultatif)			
Nom			
Prénoms			
Adresse	Rue		
	Code postal et ville		
Société d'appartenance (facultatif)			
Nom			
Prénoms			
Adresse	Rue		
	Code postal et ville		
Société d'appartenance (facultatif)			
DATE ET SIGNATURE(S) DU (DES) DEMANDEUR(S) OU DU MANDATAIRE (Nom et qualité du signataire)			
 Gérard Bonneau-Mandataire 921030			

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.